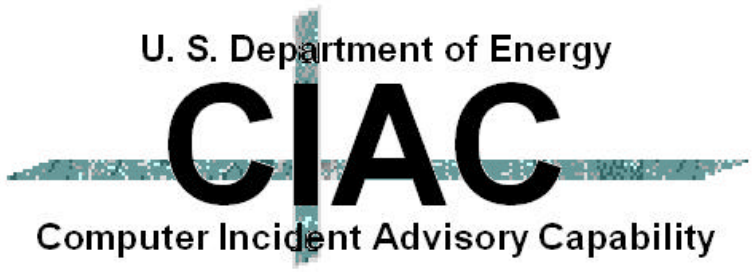


Computer Security Servers for the DOE Complex

Presented By

William J. Orvis, CIAC Team

Presented At

20th Department of Energy

Computer Security Group Training Conference

4/27/98 to 4/30/98

St. Petersburg, FL

UCRL-MI- 129569

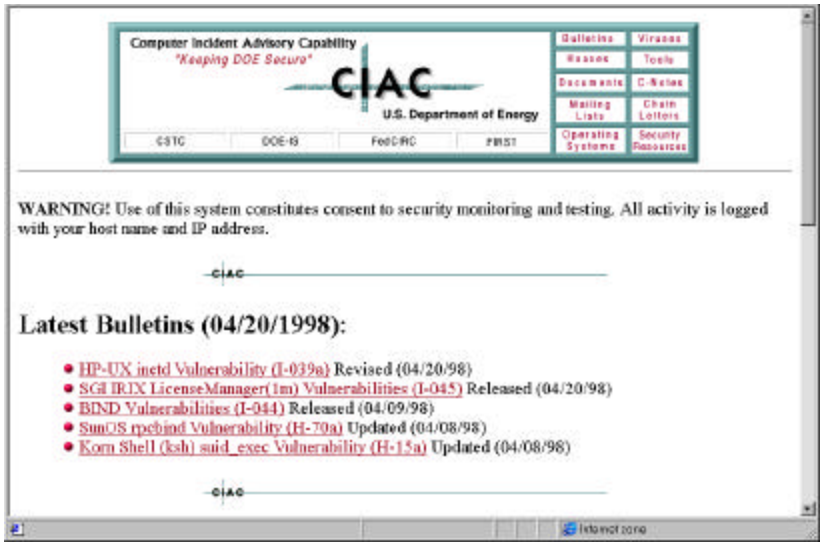
Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48

Multiple Information Servers Are Available For DOE Security

- CIAC (http://ciac.llnl.gov)
  - Bulletins
  - Virus Database
  - Security Documents
- DOE-IS (http://doe-is.llnl.gov)
  - Security Resources
  - DOE Developed Resources
  - User Needs
- DOE Secure (https://vap.llnl.gov)
  - VAP vulnerability database
  - Security Contact List
  - Documents in process
  - Bill and Rose's bad list

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

CIAC: The Latest Computer Protection Information



http://ciac.llnl.gov
anonymous server

- CIAC Bulletins
- Patch information
- Virus database
- Hoax and chain letter information
- Security documents
- Security mailing lists
- Tools (SPI, NID)

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

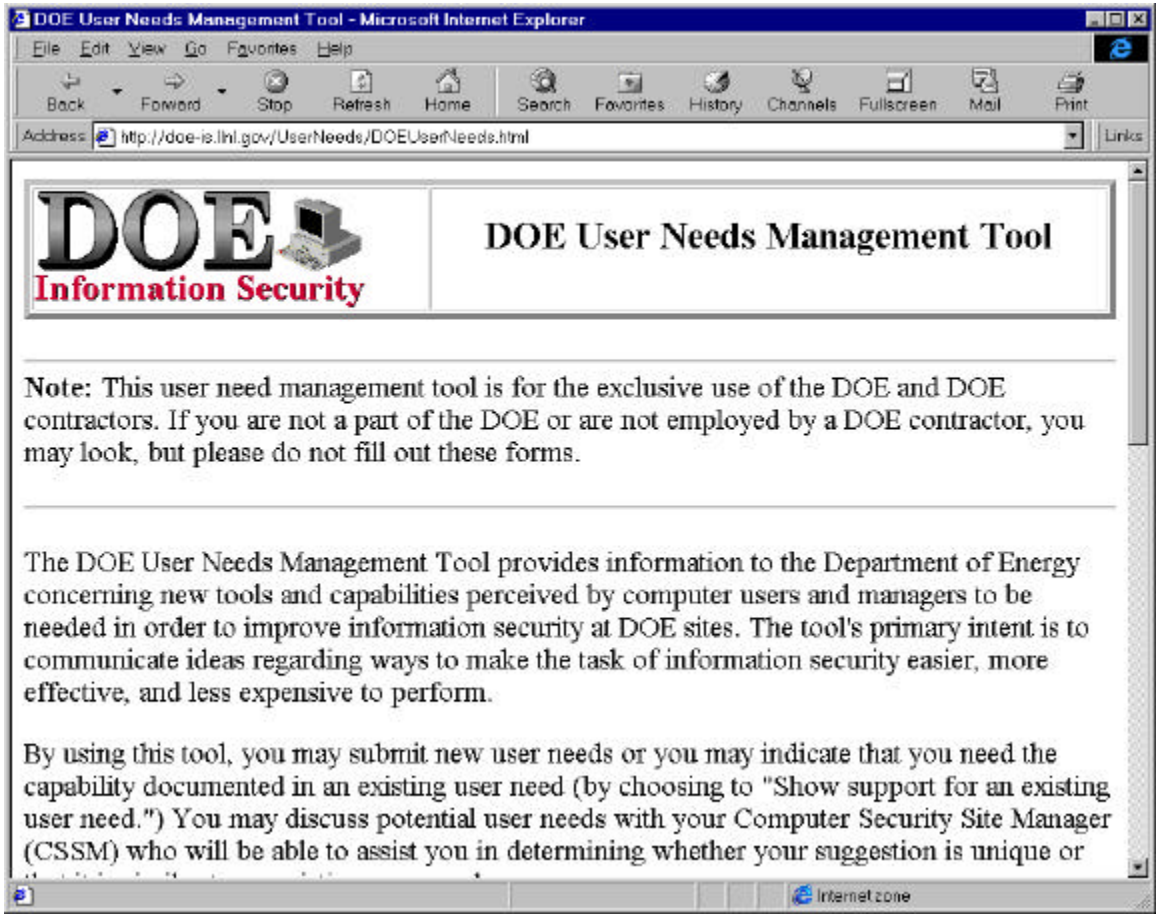
DOE-IS: Tools And Resources

http://doe-is.llnl.gov
anonymous server

- **Find information security related tools**
- **Advertise and distribute resources you have developed (tools, documents, tutorials, etc.)**
- **Tell DOE what you need (User Needs Management Tool)**

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Let DOE Know What You Need



Simple, web based form.

Give needed feedback to DOE about what is needed to improve operations and security in the field.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

DOE Secure: A Server For Protected Resources

(We need a logo.)

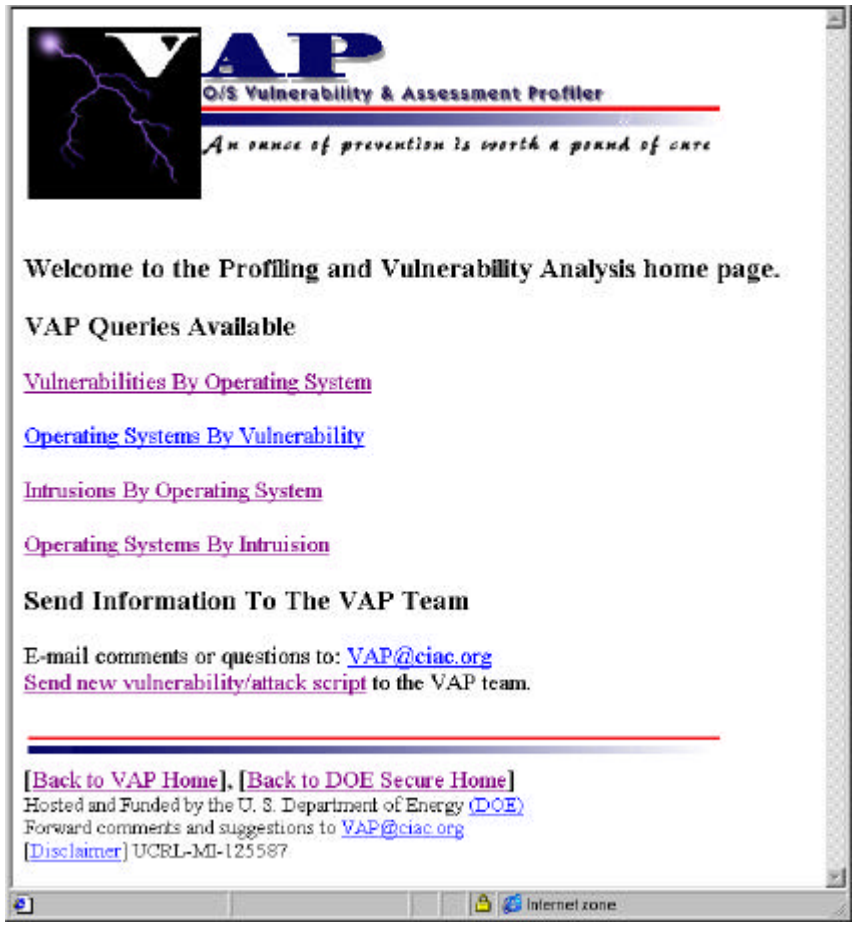
- The VAP Vulnerability Database
- Security Contacts List
- Bill and Rose's Bad List
- Draft documents for review

https://vap.llnl.gov
128 bit domestic encryption
username/password

What else would you like to see here?

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

VAP Contains Vulnerabilities And Intrusions



- **Vulnerabilities include**
  - **Vulnerable systems**
  - **Descriptions**
  - **Bulletins**
  - **Patch information**
  - **Work arounds**
- **Intrusions include:**
  - **Attack scripts**
  - **Descriptions and analysis.**

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

The User List Doubles As The Security Contacts List

- The DOE Secure user database contains contact information for all DOE security officers.
- Quickly find out who to talk to at different sites.
- Quickly generate mail, phone, and e-mail lists for different levels of security officer (CSSOs, CPPMs, etc.).

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Bill And Rose's Bad List Contains Attacking Sites

- **The list is generated from the CIAC database of current attacking sites.**
- **The list indicates what IP addresses that current attacks appear* to be coming from.**
- **Use the list to detect for related attacks and to block current attacks.**

*Note: Inclusion on this list does not mean that a site is bad, only that attacks appear to be coming from that site. The site may be compromised or its address may be spoofed.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

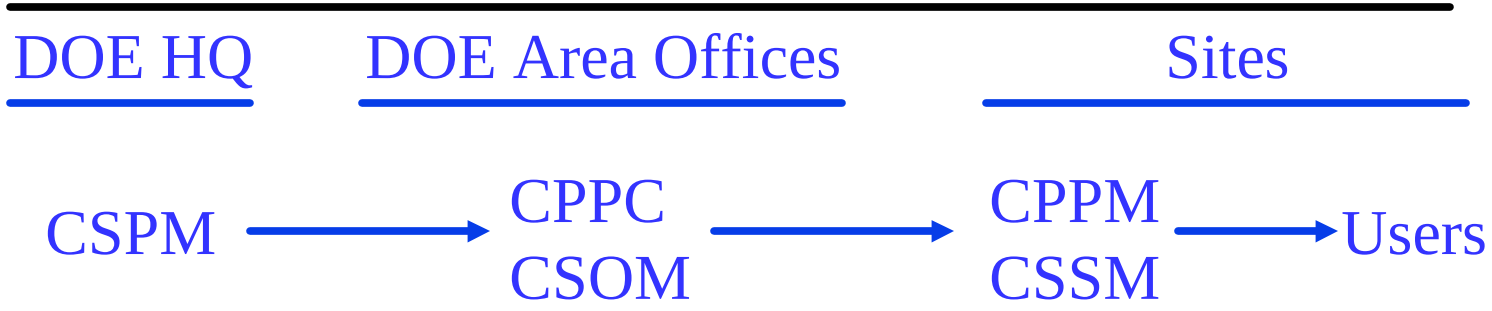
Access To DOE Secure Has Some Security Requirements

- You must use a domestic version of a web browser that has 128 bit SSL encryption.
- You must have a username and password on the system.
- Cookies must be enabled.
- You must quit your browser after using the site to delete the saved username and password.
- You must set your browser to not cache to disk any of the encrypted pages (IE) or empty the disk cache before quitting (Netscape).

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Account Creation Authority Is Local

- **Accounts are created by a hierarchy of sysops to spread the work around.**
- **Maintaining a single account gives access to DOE Secure, VAP, and maintains the security contacts lists.**
- **Access by non-DOE individuals will be on a case by case basis.**



U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Account Creation Is Simple

- Get a signed user statement (on the home page).
- Put the name, username, and password on the web based form.
  - The new user can then connect and add or update the contact information (phone, address, e-mail, etc.).
- Give the user access to any needed services (VAP) by checking boxes.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

VAP Access Requires A Second Step

- There is a second user statement for VAP access dealing with protection of the VAP data.
- An account authorizer can then give access to the vulnerabilities or to the vulnerabilities and attack scripts.
  - Access to vulnerability information, including patches and workarounds should be available to most DOE security officers.
  - Access to attack scripts should be reserved for those who need to know how a breakin occurs.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Use These Resources To Make Your Life Easier

- **Encourage all people at your sites to use the CIAC and DOE-IS public servers.**
  - **Up-to-date security bulletins.**
  - **Use the User Needs page to get needs and good ideas to the people who can do something about it.**
  - **Get credit for your tools and reports by putting them on DOE-IS.**
- **Give your computer security managers access to DOE Secure.**
  - **VAP**
  - **Contacts lists.**

Any ideas for a DOE Secure logo???

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability